BPS: Recycling Contamination Detection

Data Privacy Impact and Risk Analysis

Released version

Smart City PDX

June 30, 2025

PRIVACY ANALYSIS REPORT

City of Portland Privacy Toolkit

WHAT IS PRIVACY RISK AND IMPACT ANALYSIS?

The Privacy Impact Analysis ("PIA") is a method to quickly evaluate what are the general privacy risks of a technological solution or a specific use, transfer, or collection of data to City bureaus or offices. The PIA is a way to identify factors that contribute to privacy risks and lead to proper strategies for risk mitigation or alternatives that may even remove those identified risks.

The Privacy Impact Analysis may lead to a more comprehensive Impact Assessment and a Surveillance Assessment depending on the level or risks identified and the impacts on civil liberties or potential harm in communities.

In the interests of transparency in data collection and management, the City of Portland has committed to publishing all Privacy Assessments on an outward-facing website for public access. PIAs do not include specific uses of technology or data other than those initially evaluated.

WHEN IS PRIVACY IMPACT ANALYSIS RECOMMENDED?

A PIA is recommended when:

- A project includes surveillance technologies.
- A project, technology, data sharing agreement, or other review has been flagged as having some privacy risk due to the collection of private or sensitive data.
- A technology has a high financial impact and includes the collection, use or transfer of data by city bureaus or third parties working for or on behalf of the city.

WHAT IS IT INCLUDED IN A PRIVACY IMPACT ASSESSMENT?

City staff completes two sections included in a privacy impact assessment report:

- *The Privacy Analysis form.* This document identifies all important information related to the project description, data collection, use, safekeeping, and management; as well as verification of existing privacy policies and measures to protect private information.
- *The Privacy Risk Assessment.* This document breaks the privacy risk into six different areas of evaluation: (I) Individual Privacy Harms; (II) Equity, Disparate Community Impact; (III) Political, Reputation & Image; (IV) City Business, Quality & Infrastructure; (V) Legal & Regulatory; and (VI) Financial Impact. Then compares risks to the likelihood of happening to create a single risk measure based on the worst-case scenario.

Executive Summary

The City of Portland's Solid Waste and Recycling Division within the Bureau of Planning & Sustainability needs to make efforts to monitor and reduce the amount of non-recyclable items in recycling during at least the first four years of the State of Oregon's Plastic Pollution and Recycling Modernization Act (PPRMA). Recycling systems must also evaluate inbound material quality and contamination arriving at recycling facilities.

In industry terms, items that are not accepted within recycling at homes and businesses are considered 'contamination.' The PPRMA included requirements intended to reduce contamination in recycling because it increases costs for all customers and for entities responsible for recycling, and renders otherwise recyclable materials non-recyclable, thus reducing the environmental benefit of recycling activity. Among the anticipated allowed uses of funds to reduce contamination is the use of cameras and image recognition technology on collection trucks for the sole purpose of detecting contamination in recycling bins. Customers will be notified about any contamination in their recycling containers. Under the PPRMA, recurring and significant violations may be subject to some form of penalty.

There are four main stakeholders in this analysis: The City of Portland's solid waste and recycling program, recycling haulers, technology vendors, and customers. If adopted, customers will not have the option to decline use of this technology to detect contamination in recycling.

Privacy impacts of computer vision software applied to recycling contamination identification can include different challenges and privacy risks. Customers may develop a sense of invasiveness and uncertainty when cameras record images of their waste. The City and haulers need to make effective efforts to communicate that the sole purpose of this project is contamination detection and to inform customers about privacy safeguards. The City's solid waste and recycling program already operates a direct information hotline, coordinates with the 311 program, and provides guidance on proper recycling, to make sure customers' comments and concerns are properly addressed and to ensure customers receive accurate information and comprehensive assistance.

There are three legal considerations that should be acknowledged because of their potential impact on data collection and consent—which are aspects of privacy. One, the Supreme Court of Oregon considers a natural and legal person's trash as Private Property and warrantless searches (in any form) should be avoided. Two, the PPRMA effectively requires the City or its service providers to monitor for incorrect use of recycling systems and notify account owners. Three, the Oregon Consumer Privacy Act (OCPA) could apply to the vendor or the hauling companies. If the vendor or hauler reaches certain thresholds regarding people's data, they would be required to perform tasks to comply with these Oregon's consumer protection laws.

The following table highlights the main risks in each area of analysis.

Risk area	Risk level	Highlighted risks
Individual Privacy Harms	Medium	There are two main individual privacy risks that this assessment found: Risk of invasiveness and the risk of false notification or fine due to a false positive.

		The City needs to be very clear and effective to explain that the sole purpose of this project is to detect contamination in recycling bins. Human operators can validate contamination detection to reduce errors in identifying contaminants and ensure confidence in the systems. These human interventions can be strategically deployed based on impacts and priorities of the waste and recycling program and the hauling companies. Implementation of technology must include clear requirements and processes to discard sensitive information in footage. Collection of information should be minimized to only capture contaminants. Technology vendors may blur or reduce resolution of images shared as proof of contamination.
Equity, Disparate Community Impact	Medium	There are privacy risks that may create harm to groups or demographics. Community may lose confidence in the City's ability to use technology responsibly or assume that the City's technology will in some way harm them. Risk of bias in training data for identifying recycling items or bias in the image detection algorithm, and risk from unequal use of camera and image recognition. Risk from unequal use of technology depending on how different companies implement these technologies may create disproportionate risks to different neighborhoods. Standardization, transparency, reporting, audits, and public participation can help to identify and reduce these risks.
Political, Reputation & Image	Medium	The collection of footage may capture images of waste considered sensitive or personal. Public release of images or unauthorized access could create political and reputational harm. Additionally, there may be negative perceptions of the City's efficiency and spending priorities, if a new system is rolled out poorly or if fines are issued during a period when the city is experiencing cuts to other services. The project should ensure PDX 311 is aware of potential calls for information about cameras and data collection regarding recycling, and instructions and responses should be provided in relevant languages.
City Business, Quality & Infrastructure	Medium	Two risks are highlighted here: Risk of overall poor technology quality of service and the risk of failure to comply due to complex information systems necessary to support customers. Poor quality of service may manifest due to systemic device issues, poor installation, or low efficiency in object identification in recycling hauler trucks. Working with vendors and implementing effective operation and maintenance processes should reduce these risks.

		Implementing information technology requirements like cybersecurity and privacy protection have historically been out of scope of regular hauling operations. Efforts to transition to an information-driven operation that may include responsibilities for drivers and customer service staff, or city staff, will take time and additional resources.
Legal & Regulatory	Medium-High	Legal risks are present. If the sole purpose of the use of this technology is the detection of contamination in recycling containers, the risk from litigation is lower. If fines are given, certain data collection may be required to confirm and keep the quality of data high, which may increase the level of legal risk, that is, geolocation data, addresses, and images of recycling and/or contaminants. Additionally, harm increases if the City, vendor, or haulers get it wrong. Further, if the police want to investigate the recycling of a certain property it would be legally risky for a technology vendor, hauling companies, or city staff to provide images without a subpoena, court order, or other legal mechanism. Any information transfer to the City from companies or information requested by the City from companies and used for a City business purpose becomes public records and Portland Police will have access to it, opening the possibility to legal challenges due to the Oregon's Supreme Court decision to ban searches in individual waste without a warrant. These information and images that are public records can be publicly released in response to a public records request following public records laws. Thus, creating another avenue by which images can be shared. Consider releasing aggregated information about contamination detection to reduce the number of public records requests and to inform and educate people about this program. Systemic errors leading to unfair or undeserved fines may also be a cause of legal action.
Financial Impact	Medium	These technologies are relatively new, and some vendors may have additional costs due to hidden licensing fees or changes in the technology vendor's terms on service. Selection of a specific technology solution must consider additional modules and fees, including service, advanced algorithms, or specific support to non-standard images in training sets. Certain additional costs or investments in training hauling companies staff, including drivers and operators, on how to use these tools and on information security, the best practices might not be considered as part of the expenses in this program.

BPS: Recycling Contamination Detection Privacy Analysis

Purpose of technology, project, data sharing or application

The purpose of the technology is to analyze images of households' recycling bin contents by garbage and recycling companies (haulers) as it is collected, to identify, and notify customers about, contamination in their recycling containers. Contamination detection will be flagged to the City's Solid Waste and Recycling Program.

When recycling contamination is detected, customers will be notified by the City or haulers with information about items that don't belong in their recycling (and potentially apply fines or consequences for continuous or egregious contamination of recycling containers).

Oregon Revised Statutes (ORS) 459A.008, Expanded education and promotion program, requires that cities and counties inform generators of solid waste, including domestic households and businesses, about the benefits of reducing, reusing, recycling and composting material, promoting use of recycling services and reducing contamination in collected recyclables.

Oregon law defines "Contaminant"[1] as:

(a) A material set out for recycling collection that is not properly prepared and on the list of materials accepted for recycling collection by a recycling collection program; or

(b) A material shipped to a recycling end market that is not accepted or desired by that end market.

The State of Oregon has the commitment to reduce contamination in recycling and the Department of Environmental Quality has established goals for recycling contamination reduction.

The Oregon Plastic Pollution and Recycling Modernization Act[2] will update Oregon's outdated recycling system by building local community programs and leveraging the resources of producers to create an innovative system that works for everyone.

This act requires producers of residential and commercial packaging, printing and writing paper, and food service ware to join a Producer Responsibility Organization (PRO), and through the PRO, fund the end of life of those materials, which includes processing and recycling.

According to ORS 459A.955[3], recycling facilities are required to evaluate and report on inbound material quality and contamination. This information needs to be provided to DEQ and local governments, or local governments' service providers responsible for collecting the materials evaluated[4].

[1] https://oregon.public.law/statutes/ors_459a.863
[2] https://www.oregon.gov/deq/recycling/pages/modernizing-oregons-recycling-system.aspx
[3] https://oregon.public.law/statutes/ors_459a.955
[4] https://oregon.public.law/statutes/ors_459a.959

ORS 459A.920[5] requires contamination management fees to be paid by producer responsibility organizations to commingle recycling processing facilities to compensate for costs of removing and disposing covered products that are contaminants.

Recycling processing companies need to report on the end markets for materials. DEQ or producer organizations may disclose summarized information or aggregated data if the information or data does not identify the proprietary information of any specific processor (ORS 459A.955).

The Oregon Plastic Pollution and Recycling Modernization Act will update Oregon's outdated recycling system by building local community programs and leveraging the resources of producers to create an innovative system that works for everyone.

This act requires producers of residential and commercial packaging, printing and writing paper, and food service ware to join a Producer Responsibility Organization (PRO), and through the PRO, fund the end of life of those materials, which includes processing and recycling.

Funding from Circular Action Alliance[6], through their responsible packaging program, has primary funding agreements with local governments to support the Oregon Plastic Pollution and Recycling Modernization Act. This funding may enable recycling hauling companies to use modern technology to identify contaminants in the content of recycling bins, use this information to improve services, and inform local governments.

The Bureau of Planning and Sustainability's Solid Waste and Recycling Program is evaluating the use of hopper cameras mounted on recycling companies' trucks with image processing and object identification features to detect contamination in recycling bin loads.

The Oregon Supreme Court case State v. Lien, 364 Or. 750, 752 (Or. 2019), held that a warrantless search of a private household's garbage bin could violate their protected privacy interests under Article I, section 9 of Oregon's Constitution[7].

This project has the sole purpose of identifying contaminants in recycling bins, with no intention or ability to identify personal identifiable information from the recycling bins content, or the recycling user's privacy rights. Hauling companies will collect information to identify the household owner of the recycling account.

Name of the entity owner of the application and website

A part of the project is to identify equipment ownership. This assessment covers the scenario where recycling hauling companies or the City of Portland own the equipment and service. This includes equipment, contracting, information, sharing agreements, and accounts accessing video recordings, pictures and screen captures taken in the identification process, and metadata that includes geolocation and customer information.

[5] https://oregon.public.law/statutes/ors_459a.920

[6] https://circularactionalliance.org/circular-action-alliance-oregon#ORSOP

[7] Article I, section 9, of the Oregon Constitution provides, in part, that "[n]o law shall violate the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable search, or seizure[.]".

Ownership of equipment is still part of the planning analysis for this project. Most financial risks depend on who absorbs costs derived from them. Privacy risks center on the information involved and who has access to it, which is independent of who owns the technology, but rather how it is used.

The City of Portland's Bureau of Planning and Sustainability's Solid Waste and Recycling Program will offer financial assistance to purchase technology (devices and information management systems) that need to comply with minimum technical requirements, including cybersecurity, privacy protection, data governance, etc.

Currently, the hauling companies include PDR, Arrow/City Sanitary, Walker, COR, Republic, Recology Clackamas, Heiberg, and WM. For information about companies permitted to offer recycling services in Portland, visit:

https://www.portland.gov/bps/garbage-recycling/permitted-commercial-garbage-and-recycling-companies

To learn more about the City of Portland's Garbage, Recycling, and Compost program, visit:

https://www.portland.gov/bps/garbage-recycling

Type of Organization

Public-Private

Scope of personal data collected. List all sources of data and information.

The following description of data and information is based on an initial survey sent to recycling companies to understand how they are using hopper cameras and the ways in which these systems can be upgraded with image processing and object identification for contamination detection.

Data

- Images showing recycling contents from residents, commercial, and multifamily customers.
- Geolocation information or other methods that determine the address of the recycling pick up.
- Customer data applicable to the recycling service.

Sources

- Camera
- Onboard geolocation system.
- Direct input from driver or hauler companies' employees.

How personal data is collected, and its frequency.

At the time of this assessment, this analysis assumes that images of recycling are collected by onboard camera systems and image recognition tools. A camera is pointed toward the falling recycling materials and captures images. This results in images of discarded materials linked with the owner's account information (e.g., utility payment status, address, etc.).

Who can access the data?

There are three stakeholders in this use case: City of Portland's Solid Waste and Recycling Division, recycling hauling companies, and the technology vendor offering the image detection system. Some information is anticipated to be accessible to customers, particularly when contamination has been detected, and they are notified.

The vendor may collect information about the contents of recycling collected from residents, commercial, and multifamily customers.

Recycling hauling companies or the technology vendors would collect images, image identification data, and metadata, using monitors to view and flag recycling contamination, and to review flagged collections, including type of contamination, location and time. The image recognition vendor may uptake video from the cameras. It may also do it in a certain way depending on whether image recognition will occur during the collection, in real-time, or later. There are camera systems onboard the trucks that are not sent to the vendor for object detection but are used for the protection of the truck and its driver (these cameras are not being assessed in this).

The City may reserve a right to access data for inspection, compliance, or auditing purposes. However, such data may become public record after inspection or use. This action should be done with caution.

A public record is one that is "prepared, owned, used or retained" by the City. So, the program could be required to produce records that are used even if the Bureau did not create them and is not storing.

Purposes the data is used for

The data collected would ultimately be used to identify and notify customers of items that do not belong to their recycling and potentially apply fines or consequences for continuing and egregious use of recycling containers.

Currently, when a driver identifies contamination, they may leave a tag on the user's recycling bin. Recycling hauling companies may use recorded images to identify contamination and improve their services. Data can be used for reporting, evaluating the use and effectiveness of technology, or for auditing purposes by the City, the recycling hauling companies, or authorized third parties.

Where the data is stored

It is not fully defined what data will be stored by whom at this research stage of this project. While it is early in the procurement process, this assessment can inform decisions about information management and technology.

Information collected by the City of Portland may be stored in the City's servers and follow existing public records laws, information security policies and procedures followed by the City, open data practices, and mandatory reporting required by law and funding sources.

Video footage captured by hopper cameras may be stored in the device, hauling company servers, and/or technology vendor servers, depending on the services selected for this project and privacy-preserving choices.

Additional metadata, including geolocation information, notes or flags reported by the driver or recycling company staff reviewing the footage, and other derivative information, would likely be stored under the recycling company's ownership. The City of Portland will likely not have access to this information, except when requested for the purposes listed above.

How data is shared

At the time of this assessment, this analysis assumes that information is collected by cameras on recycling trucks and processed by technology vendors. Information will be shared with the City of Portland and include household specific incidents and other aggregated information about recycling contamination detection management. The City of Portland (or haulers if authorized by the City) may provide feedback to customers and issue fines or fees to specific households based on existing laws in Oregon or the City of Portland.

How long is the data stored?

The image identification service vendor may have its own retention schedule according to their own Terms of Use. The recycling company may have different retention times for information managed by them. The City of Portland will follow legal requirements defined for this type of record.

Effectiveness

Camera effectiveness and an image processing algorithm's effectiveness depend on several factors depending on the technology, the ongoing maintenance, or how it is used.

The object identification technology depends on multiple technical and physical factors including training sets, algorithm, the quality of the camera and lenses, lighting, image capture speeds, etc. Environmental conditions including weather, temperature, visibility, etc. may affect true-positive and rates.

A confusion matrix is a simple table that shows how well a classification model is performing by comparing its predictions to the actual results. It breaks down the predictions into four categories: correct predictions for both classes (true positives and true negatives) and incorrect predictions (false positives and false negatives).

In image recognition, a confusion matrix can be described as follows:

True Positive (TP) - An accurate detection where the object detection model correctly recognizes and locates objects, with the geometry detection between the predicted bounding box and the ground truth bounding box meeting or exceeding a predetermined threshold.

True Negative (TN) - Not used in object detection because it focuses on accurately confirming the absence of objects.

False Positive (FP) - An inaccurate detection, when the model mistakenly identifies an object that is not present in the ground truth or when the predicted bounding box has a geometry detection below the specified threshold.

False Negative (FN) - Failure to detect ground truth, when the model doesn't identify an object present in the ground truth, essentially indicating that it overlooks these objects.

Necessity & Proportionality, Fundamental Rights, and Consent

Necessity and Proportionality

Our use of the term "Proportionality and Necessity" refers to whether the means of collection and the data collected are necessary to complete a specified aim, that is, not collecting, retaining, or sharing more information than necessary to notify account owners of proper recycling; and to consider if there are less intrusive but equally effective ways to complete the specified aim. In other words, analyze whether technology is proportional to the objective. Technology could be said to be proportional if the data used does not pose an outsized privacy risk compared to the benefits gained from this technology.

The contents of people's recycling should be treated with care because images of non-authorized items in their recycling would be linked with their name, address, or other information related to the provision of waste collection services (if individualized notice or fines are given).

It is unclear whether legacy camera and driver monitoring systems (without image recognition) are better at detecting and removing contaminants than human inspection, however, it is likely that the image recognition system will improve both rates to some degree. Mainly, by indicating some contamination that a driver may not notice.

Vendors should provide metrics about the effectiveness of their technology. More research should be done on its effectiveness once a vendor has been selected. An image recognition system may not be necessary, but given proper privacy and AI risk controls, it may be proportionate to its purpose.

It may become an issue when there is unintentional sharing via public records requests and informal police requests. Many customers and community members may have an expectation that whatever is thrown out is not rifled through by police, City, or some other organization, while many others may believe that whatever is put out on the street is free for rifling. However, most don't expect it to be shared outside of the hauling company either. The City of Portland intends to serve the community, and processes handling data should align with the expectations and goals established for this purpose.

Consent

Because the City is required to provide or assist in providing feedback, there is no consent mechanism that would allow homeowners or organizations to opt out of being informed of incorrect recycling behaviors.

There still may be an opt-out mechanism for the *use* of image recognition or computer vision; pragmatically, if the level of ethical risk generated from this technology is low, then an opt-out

mechanism may not be necessary to or worth creating and maintaining. If the level of ethical risk generated is not low, then these services may need to explore opt-out (or potentially opt-in) mechanisms.

Things that contribute, largely, to ethical risk are the accuracy of the model and whether there will be a fine. Additional ethical risks stemming from false positives and false negatives may appear as this technology gets implemented.

Privacy safeguards

Data Minimization: Camera is fixed toward falling/fallen materials leaving a recycling container. Data collection should be monitored only for the purpose of identifying contaminants in hauling company customer's recycling bin.

Use Limitation: Use is limited only to performing the recycling contamination detection.

Open source

No.

AI/ML claims

Computer Vision/Image Recognition/object detection/image detection.

Privacy Policy (link)

N/A

Surveillance Tech?

Yes. Individuals have a privacy interest in the waste materials they place in trash according to the Oregon Supreme Court, and at the same time the public has an interest in appropriate use of the recycling system. Because the project's purpose is to notify people of incorrect sorting, their recycling will be connected to their home/organization address and a respective name or account. This project is monitoring the activity of a natural or legal person.

Individuals have a privacy interest in the waste materials they place in trash according to the Oregon Supreme Court, and at the same time the public has an interest in appropriate use of the recycling system.

Portland Privacy Principles (P3)

Data Utility: All information and data processes must bring value to the City of Portland and the communities the City serves. The City will collect only the minimum amount of personal information to fulfill a well-defined purpose and in a manner that is consistent with the context in which it will be used.

Image recognition technology has the potential to increase recycling and reduce pollution by minimizing contamination in recycling bins and encouraging private households and businesses to learn more about what materials can be recycled in Oregon. Because contaminants affect the recyclability of other recyclables, it is important to avoid contamination. The project will support optimal collection of recyclable materials, thus saving time and recycling more materials.

Data collection and retention will be minimized to the quality and quantity necessary for the completion of the project's aim. A project to install contamination reduction cameras would not collect more information in type or quantity than is already collected via cameras already stationed on many trucks. In this "legacy process" a camera is connected to a monitor displayed to drivers so they can detect any falling contaminants. For some haulers, the system allows playback so the driver can view the contaminant and for other haulers someone in their offices may review the tape for contaminants.

Image recognition instead generates metadata from images—what the objects in the recycling are and whether there is a contaminant. The hope is to either decrease the rate at which contaminants slip past drivers or replace this task, so drivers won't need to review each bin.

The best choice for data minimization is to let haulers notify and the vendors collect -- avoiding unnecessary data transfer to the City entirely or as much as possible. In this scenario, this assessment recommends limiting the purpose of detecting contamination in recycling bins and limiting information sharing to only the required information to the City and stakeholders involved in this process, false positive detection, security, and redress.

Full Lifecycle Stewardship: Data, Metadata and Information will be secured and protected throughout its life cycle. That includes collection, storage, use, control, processing, publication, transfer, retention and disposition.

The data and processing details in this project are unclear as it is still in development, however, there are security standards that anyone working on behalf or request from the City should uphold. Additionally, the vendor or hauler may need to comply with obligations in the Oregon Consumer Privacy Act (OCPA) which also provides account holders with certain rights related to their data, if they meet specific account and data selling thresholds.

It may be beneficial for the City of Portland to retain as little information as possible and leave much (if not all) of the processing of data to the vendor and the hauling companies. The vendor provides the image detection software service. There have been pilots of this kind of technology for contaminant detection, particularly in Michigan[8], in which the vendor was able to blur the image, leaving just the contaminant in the frame; and is thus used for notifying account holders of improper recycling. In a scenario where the city minimizes its collection of data, the hauling companies are ostensibly the entity that would notify the account holder when contaminants are identified.

It may be necessary given the Supreme Court ruling and the recent precedent set by Lien v. State, that the haulers and vendors should avoid providing images of recycling, blurred or unblurred, to the Portland Police Bureau without a judiciary warrant, to prevent litigation.

Transparency and accountability: How the City uses, manages and collects information is described clearly, accurately, and shared in an accessible way. Who creates, contributes to, and has access to that information is also clearly documented and communicated to all people who entrust city government with their data and information.

Consent by users is not required by state law and the program would not work if there was an opt-out mechanism. Like other technologies such as speeding cameras, the use of cameras and computer vision is of the public interest with a particular purpose of public wellbeing. Although consent will not be obtained by account holders, an opt-out mechanism was considered for the use of computer vision and an opt-out of having an image of contamination be used in the household feedback notice.

The waste and recycling program may consider developing a notice in conjunction with haulers indicating that the haulers will be using cameras, computer vision, and that images of contaminants may be used to inform account holders.

While this application of computer vision holds lower risk than other areas like health care or criminal justice, the City shouldn't dismiss account holders' potential concerns on the basis that it is a low privacy risk use case. The project should implement administrative or technological structures to ensure that the technology is doing what it is supposed to be doing—accountability—including human-in-the loop, algorithm auditing, and explainability.

[8] https://www.kalamazoocity.org/News-articles/Kalamazoo-Launches-High-Tech-Contamination-Reduction-Campaign-This-Month-For-Nearly-14000-Households

The program can develop systems for feedback, course correction, and redress just in case incidents with the technology or the application of it appear. The city's customer service staff play an important role in handling requests for information and assistance.

Ethical and Non-Discriminatory Use of Data: The City of Portland has an ethical responsibility to provide good and fair stewardship of data and information, following existing non-discriminatory protections, and commits to due diligence to understand the impacts of unintended consequences.

Community members should trust that the City of Portland is looking after their basic needs and interests since it enables their ability to live their lives at a certain level of quality of life. The City can ensure that data and technology minimize harm, or wrongdoing, to individuals or communities. This includes avoiding use of data for other purposes besides the one specified. All agreements with haulers and vendors should reflect this.

If the City intends to fine or allow a hauler to assess a fee on an individual account, the account holder should be informed and notified in advance. So, this assessment ought to review how contamination detection is linked to the account holder and the project should ensure that sufficient proof is available in assigning contamination to an account.

Data Openness: Data, metadata and information managed by the City of Portland -- and by third parties working on behalf of the City -- that are made accessible to the public must comply with all applicable legal requirements and not expose any confidential, restricted, private, Personal Information or aggregated data that may put communities, individuals, or sensitive assets at risk.

Images of people's recycling may be categorized as restricted or non-restricted. In this data category they are retrievable by community members via an approved public records request. Avoiding sharing images to the City of Portland and allowing it to remain with hauling companies (with an understanding that they have appropriate privacy and security measures themselves) can improve information protection.

Informing the public about recycling contamination detection incidents in aggregated form can also showcase the effectiveness of this program. Access to data in open form in dashboards or raw tables can enable communities to identify their own issues and encourage civic participation in this program.

Equitable Data Management: The City of Portland will prioritize the needs of marginalized communities regarding data and Information management, which must be considered when designing or implementing programs, services, and policies.

Stakeholders: Vendor, Haulers, City of Portland's Solid Waste and Recycling Program, and Account Holders (e.g., homeowners, multifamily dwellings, businesses, organizations).

Marginalized communities, whether homeowners or residents of multifamily buildings, could experience disproportionate fines if they lack equitable access to information about recycling or if they lack convenient, sufficient access to sort their discarded materials properly. Another

example of an important equity question is the appropriate level of financial penalties, if any, assigned to accounts with significant contamination. For example, and only for example, will a homeowner be fined at the same rate as a business? Could a co-op or landlord unjustly inflate fines to generate additional revenue from tenants?

Automated Decision Systems: The City will create procedures for reviewing, sharing, assessing, and evaluating City Automated Decision System tools -- including technologies referred to as artificial intelligence -- through the lens of equity, fairness, transparency, and accountability.

Harm or wrong may occur where the system is inaccurate in identifying items that are not recyclable. Or where the City, haulers, or vendor are not transparent, accountable, or fair. Notice should be given to accountholders about the project and about the use of AI.

Contamination detection vendors should provide metrics for quality control and for constant improvement to minimize false positives and improve detection rates. Vendors may have the ability to implement an ongoing improvement program to add new training datasets to improve identification rates.

Privacy Impact Risk Severity Assessment

WORST CASE SCENARIO	Medium

Baseline (B): (T) – Technology level, (U) – use and application level. Risk type (RT): (I) Individual Privacy Harms; (II) Equity, Disparate Community Impact; (III) Political, Reputation & Image; (IV) City Business, Quality & Infrastructure; (V) Legal & Regulatory; and (VI) Financial Impact.

B	RT	Risk description	Impact	Likelihood	Mitigation, comments, and strategies	Risk level
T	I	1.1 Risk of over reliance on computer vision	Low	Possible	Automated object identification systems may create a sense of perfect efficiency; however, misidentification errors can appear, despite having someone in the loop, driver or someone else, who could verify the computer vision's decision. Allowing the algorithm to decide what contamination is without a human review mechanism will lead to mistaken decisions downstream. Ensure people in the loop to validate outcomes of the automated detection system. Also, encourage hauling companies or technology vendors to keep metrics that measure false positive detections and report aggregated data about efficiencies of these services.	Low
U	I	1.2 Risk of unauthorized sharing or use of images	Moderate	unlikely	Some images, particularly printed materials, may contain name, personal address, or even sensitive information like medical or financial materials. High-definition images and high-speed cameras may be able to capture this type of information. It is important to nurture a culture of information protection and personal responsibility on personal information disposed of recycling. Depending on whether the image is deidentified, that is, not linked with any name or address, the impact will be lower. The City should set information protection expectations to recycling hauling companies to protect personal information included in recycling bins.	Low
U	I	1.3 Risk of not Informing customers about these services	Moderate	unlikely	The risk of not informing recycling companies' customers about contaminants detected and potential violations is a risk of not being transparent.	Low

B	RT	Risk description	Impact	Likelihood	Mitigation, comments, and strategies	Risk level
					Customers should have active and effective channels to provide input and request information about these services. These channels can be offered by the City of Portland and the recycling hauling companies.	
T	I	1.4 Risk of public mistrust due to not providing opt-out/opt-in options	Low	Likely	There is no opt-out or opt-in consent mechanism for this project, particularly from not being notified of incorrect recycling and from the use of cameras and an object/image detection system for contamination. The use of this technology has the goal to comply with existing laws in Oregon. Mitigation of the resulting mistrust can be done by properly informing households and recycling service account owners that goals of using this technology and what privacy safeguard efforts are implemented to protect people's personal and sensitive information.	Low
U	I	1.5 Risk of false notification or fine due to a false positive	Moderate	Likely	The impact of a false notification and especially a fine would harm individuals financially or by using their time without justification. The image recognition system is not 100% accurate and false positives will appear. The process should include several stages to verify a positive identification from an automated system and keep a record of it to validate it. Adding a human in the loop of validation is important. There are still false positive cases showing up even with people in the middle verifying positive identifications. The customer should have a way to verify by themselves the contamination detection and be able to challenge and fix an erroneous outcome.	Medium
U	I	1.6 Risk of a sense of invasiveness of privacy	Moderate	Likely	People can feel a sense of invasiveness of privacy, even when the systems could be fully automatic, due to a mistrust in those who have access to the recycling bins. This sentiment may be multiplied by the fact that the is no options to opt out or opt in of this service. Implementation of technology must include clear processes to discard sensitive information in footage. Recordings should be minimized to	Medium

B	RT	Risk description	Impact	Likelihood	Mitigation, comments, and strategies	Risk level
					only capture contaminants. Technology vendors may blur or reduce resolution of images shared as proof of contamination detection incidents. The City and Recycling hauling companies need to properly work on building privacy safeguards, oversight methods, and informing customers and households that the sole purpose of this technology is for identifying contamination in recycling materials. The City will need to work with its customer service staff to respond to public inquiries about this service in general and specific cases. Collecting metrics around these public inquiries and service calls can inform future improvements in privacy safeguards and communications.	
U	I	1.7 Risk of Identification or Re-identification of individual's information	Low	Unlikely	If the images of recycling and contamination are not linked with their account, say for training the contamination detection system, there is still a chance of identification or reidentification. For example, say that there is a high chance that a certain contamination belongs to a certain company or establishment (given it is not completely apparent). Or recycling is strongly correlated with a certain population. The ways unauthorized people obtain these images are risks already covered in other points, such as 'data breach' or 'unauthorized sharing'. This risk is highly reduced when all the recycling is mixed or privacy enhancing techniques are implemented in footage or image collection and management.	Low
T	II	2.1 Risk of bias in training data for identifying recycling items or bias in the image detection algorithm	Moderate	Possible	Factors that make up for this risk are mainly from the training data set and the training the machine learning model goes through before it is deployed. If the system is better at identifying unauthorized objects from minorities' recycling bins than unauthorized objects from another groups (or vice versa), then the City may give fines or notices inequitably.	Medium

B	RT	Risk description	Impact	Likelihood	Mitigation, comments, and strategies	Risk level
					The likelihood of this occurring is possible due to the large variety of objects to be identified; however, its impact is relatively moderate (notice or fine) especially if haulers have a redress system. Systemic bias may lead to high impacts in the long term. A process of constant improvement implemented by the technology vendor is recommended.	
T	II	2.2 Risk from unequal use of technology due to companies' uneven implementation.	High	Possible	Haulers may use different vendors and type of cameras (e.g., quality, brand, etc.). Because they cover different parts of Portland, it can create differences between neighborhoods recycling collection services could create disparities in how actions from contamination detection are implemented. Implementation of technology needs to fulfill a baseline or standards defining quality of services and privacy and cybersecurity safeguards. Collection of metrics that report back technology effectiveness (false positives, identifying the type of contamination), contamination detection aggregated by geography. Releasing a dashboard accessible publicly with information about contamination identification and false positives or other relevant issues can create visibility on some potential issues derived from uneven quality of vendors' technology solutions. This risk is reduced if the City has control over the technology offered by vendors.	Medium
U	II	2.3 Risk of uneven access to information by users	Moderate	Possible	Certain customers from certain neighborhoods may have better access or ability to access information about these contamination detection inspections. This could be connected to existing socioeconomic differences and systemic issues. The initial step is to make customers aware of the purpose and use of this technology. This effort should include training focus on supporting customer services through the city's customer service staff.	Medium

B	RT	Risk description	Impact	Likelihood	Mitigation, comments, and strategies	Risk level
					Staff monitoring and public bodies the recycling hauler companies should make larger efforts to include low income and underserved neighborhoods.	
T	II	2.4 Risk of undermining community trust	Moderate	Possible	The compounding of several privacy and public trust issues that can include a sense of disempowerment due to the lack of options to decline participation in this technology, potential delays on information, failures of the technology, or even previous or existing issues on the specific recycling and waste management service, can undermine community trust. It is important to consider meaningful engagement and communications strategy to inform customers about the benefits and safeguard build in this technology, and the role that the City and recycling hauler companies will play. The city's customer service staff needs to be engaged early to support properly and in a timely manner all public inquiries.	Medium
U	II	2.5 Risk of inequity from driver task saturation	Low	Possible	Depending on the type of solution and on-site responsibilities, drivers of garbage collection trucks may need to be aware of their driving, other's driving, along with their main task of collecting trash and recycling and placing it into the truck in various ways. This project increases the responsibilities for drivers and hauling trucks operators. They need to look for fallen debris in trucks, look at the object detection system to see if it picked up anything, and supervise the object detection system. Drivers could be overburdened with tasks. Drivers need to be properly trained, and their supervisors and operations planners can design processes that avoid conflicting tasks, operator distractions, and slow down their regular routes. The recycling and waste management program can work with hauling companies to make them aware of these risks connected to the expansion of the role of drivers and operators and explore alternatives that resolve these issues.	Low

B	RT	Risk description	Impact	Likelihood	Mitigation, comments, and strategies	Risk level
T	III	3.1 Images of sensitive personal garbage may be collected and shared in notifications	Moderate	Possible	Images of sensitive personal recycling bins content could be collected and used for notification. For example, a personal care item could cause embarrassment if its image is used to notify the account owner. It is important to understand that this project has a sole purpose of identifying contamination and any description of these contaminants may create a privacy risk. Alternative notification schemas may be explored, where unedited images stay only at the recycling hauler company's information management system and enable authorized access to their customers on demand. While the City of Portland only will keep metadata on detection and not footage nor image capture files. This may create an additional burden on companies and third-party personal information management solutions may be needed.	Medium
U	III	3.2 Systemic errors in detection may impact reputation of City services and recycling hauling companies	Moderate	unlikely	Image recognition technologies are still very sensitive to environmental conditions and multiple other technical factors that can impact their effectiveness. If certain errors or issues are not quicky fixed, systemic errors start to be an important factor that may reduce public trust in the technology and the service overall. Recycling hauler companies need to be prepared and work with the technology vendor to resolve any technical issues as soon as possible. This may increase their ongoing maintenance and service costs. The City also needs to work with the city customer service staff to quickly resolve public inquiries and comments. Potentially, the City may set a procedure to track these issues as they emerge until their resolution.	Low
U	III	3.3 Unattended privacy or algorithmic issues may impact program credibility	Moderate	unlikely	Customers of recycling haulers may report privacy concerns or issues to the City, either via the 311 program or directly contacting the Solid Waste and Recycling program's customer service staff. The contamination detection service and the service providers, including	Low

B	RT	Risk description	Impact	Likelihood	Mitigation, comments, and strategies	Risk level
					the City, may be impacted if these issues or concerns are left unresolved. Clear public communications about the purpose and implementation of this program and new services can help to resolve privacy and algorithmic concerns even before they arise. Prompt responses to public inquiries will help to increase credibility and support this program. These strategies can also educate Portlanders about proper recycling and increase overall performance.	
T	IV	4.1 Risk of Data Breach	Moderate	unlikely	Data breaches occur when unauthorized data sharing happens. Serious data breaches of private and sensitive information need to be reported to the State of Oregon. This project is not expected to collect sensitive information from customers, contamination detection, or metadata collection. Data breach in this case may include personal information, metadata, or information collected from devices in the hauler trucks. Hauler companies need to comply with minimum cybersecurity practices around information management, particularly customer data. These techniques may include data encryption, limiting access to information to staff, using secure channels for sharing data with the City and other authorized users.	Low
T	IV	4.2 Risk of identifying acceptable material as contamination	Moderate	Possible	Identifying contamination in recycling bins is the sole purpose of this project. These cases can be referred to as *false positives* and can directly lead to impacts to individual people, including economic fines, personal reputation, and stress connected to a non-existing violation. In addition, systemic false positives will impact public trust and credibility in this technology or the goals, creating further economic impacts due to maintenance or replacement of equipment or software. Several strategies can be useful to minimize *false positives*: • Try small-scale pilots to test new vendors. • Keep controls and monitor over misidentification of contamination,	Medium

B	RT	Risk description	Impact	Likelihood	Mitigation, comments, and strategies	Risk level
					• Request performance tests from technology vendors before acquiring or using the technology. • Include a human-in-the-loop to validate contamination detection events. • Train staff in footage collection and contamination detection procedures to manage false positive events. • Keep constant communications with technology vendors and inform them when a false positive occurs. • Include third party audits if necessary.	
U	IV	4.3 Risk of identifying contamination as acceptable material	Low	Possible	Missing contamination detection in recycling bins is a *false negative* event. Missing object identification depends on several factors including the specific algorithm used for detection; environmental conditions like lighting, distances, or particles in the air; the condition of the equipment, including optics, rates of video capture, or processors capacity; and specific collection-time conditions like obstructions or too many objects passing simultaneously. The missed contaminant will end up mixed with a recycling load and a post event analysis can provide insights on the causes for missing identification. Constant recording of a load may help to identify the problem; however, keeping that recording too long may create new privacy risks. If possible, either the hauler company or the technology vendor may be responsible for reporting and/or resolving missing identification of contaminants. Assigning procedures to manage these cases can also reduce the false negatives and identify patterns.	Low
T	IV	4.4 Risk of systemic malfunctioning equipment	Moderate	Unlikely	Electronic and optical equipment are delicate devices. Being exposed to waste, vibrations, dust, humidity, and temperature extremes may impact these devices' performance. Systemic issues are repeatable and intrinsic to specific failure modes in equipment. These issues can be inherent to the technology or	Low

B	RT	Risk description	Impact	Likelihood	Mitigation, comments, and strategies	Risk level
					connected to its implementation. In the first case, the technology vendor needs to assume responsibility for resolving or providing service and support to resolve it. Systemic issues due to how technology is implemented depends on where cameras are located, type of lighting, mounting brackets, connecting cable and power supply. Technology vendors should provide clear use and installation procedures to avoid systemic errors. The algorithm used for detecting objects can have systemic issues like bias or coding issues. Comprehensive documentation and staff training in installation, use, and maintenance procedures of equipment and software can reduce and help resolve systemic equipment issues. Constant communication with vendors can help resolve issues in the field.	
U	IV	4.5 Risk of operators misusing equipment	Moderate	unlikely	Operators can intentionally or unintentionally misuse the equipment or use it for a different purpose than identifying contamination in the recycling bins. Training operators on proper use of this technology, addition of notes and metadata part of the process of identification of contaminants and properly reporting any detected false positives or false negatives as soon as possible will reduce the risk of potential misuse. Operators' supervisors can play an important role in monitoring any potential misuse of the technology. Early identification of misuses facilitates corrections and reduces other errors. In the case of intentional misuse or abuse of the equipment, faster interventions lead to reducing any potential harm derived from it. The hauler companies and vendors need to report to the City any identified abuse of this technology.	Low

B	RT	Risk description	Impact	Likelihood	Mitigation, comments, and strategies	Risk level
U	IV	4.6 Risk of operators or other staff obtaining unauthorized access or misusing the recordings	Moderate	unlikely	Similarly to misuse of equipment, having unauthorized access to information can create other risks including information breach, personal harms, and impacts in public trust. Technology vendors can offer ways to restrict access to specific modules or operations of the contaminant detection system; while hauler companies can train supervisors on information protection best practices that safeguard information.	Low
U	IV	4.7 Risk of vandalism or stolen equipment	Moderate	unlikely	Because waste is collected in public areas such as roads or sidewalks, it is possible for a truck to be vandalized and have its equipment stolen. Hauler companies can install this sensitive equipment protected from vandalism or thief as much as possible. These physical protection measures can increase the cost of installation and maintenance but reduce the risk of property damage. For more expensive equipment, hauler companies may include them under their property insurance.	Low
T	IV	4.8 Risk of cybersecurity breach	Moderate	unlikely	Some equipment may wirelessly share information to remote servers or devices. Although, most technology vendors already implement at least basic cybersecurity standards, there is always a possibility that passwords or mobile devices with recordings or access keys can be lost. Hauler companies need to follow basic training of information protection best practices to operators and supervisors. Companies need to report any cybersecurity breach to the City to remediate any potential damage and reduce the risk of similar incidents in the future.	Low
U	IV	4.9 Risk of overall poor technology quality of service by technology vendor	Moderate	Possible	This risk can include lack of vendor support, unreliable detection, lack of response for fixing issues. Hauler companies can start pilot periods of using a specific vendor's technology to evaluate their service and technology performance in the field.	Medium

B	RT	Risk description	Impact	Likelihood	Mitigation, comments, and strategies	Risk level
					Supervisor can be trained in assessing the quality of service of these devices and services. Any lack of support can be noted and shared with the City.	
T	IV	4.10 Risk of failure to comply due to complex information systems to support customer.	Moderate	Possible	These technologies can be something new to hauler companies and their complexity involving information management, legal compliance, and reporting requirements can be too much of a burden for their regular operations. These new demands can also require additional costs, several training sessions for staff, and the development of new processes and internal policies. The City of Portland can collaborate with hauler companies by staging the deployment and use of these automatic contaminant identification systems. Limited term pilots, collaborations with vendors, and support from third parties can facilitate the long-term success of this implementation.	Medium
T	IV	4.11 Risks of backdoor access to information from vendors	Moderate	Possible	Some technology vendors terms of use allow them to use customer's data for other purposes, including improving their own algorithms, creating training datasets, or even for marketing, research, or monetization purposes. Hauler companies need to make sure that technology vendors terms of use agree with the City of Portland requirements on customers information protection. Hauler companies need to make sure that the sole purpose of the information collection is for recycling bin contaminant identification.	Medium
U	V	5.1 Risk of lawsuit due to intrusive inspection of waste	High	Possible	The sense of privacy will be present in some customers. There might be cases where some customers may start legal action against the use of this technology. The City and hauler companies need to work together on informing customers that **the sole purpose** of this technology is contaminant detection in recycling bins and offer publicly accessible information	Medium

B	RT	Risk description	Impact	Likelihood	Mitigation, comments, and strategies	Risk level
					about this program, including a description of how the City of Portland and hauler companies are safeguarding customers' privacy. In addition, the City's waste and recycling customer service staff or 311 program can become an excellent point of contact and information for those customers that want to learn more about this project.	
T	V	5.2 Risk of legal actions against the City due to systemic image recognition errors	Moderate	unlikely	This risk refers to the case where systemic and unchecked false positives end in unfair fines to customers, triggering legal action against the City or the hauler companies. The hauler companies need to be able to identify those false positive cases early on and include human-in-the-loop approaches to verify correct contaminant identification. The ability to promptly correct mistakes will include public trust also.	Low
U	V	5.3 Legal risks due to a data breach	Moderate	unlikely	Cases of data breaches that are purposely hidden from customers and the City may trigger legal actions and damage claims. Transparency and prompt action in cases of data breaches are the best way to mitigate this issue. Companies should evaluate the level of information lost. This case may include footage of recycling bins, personal information from customers or staff. No sensitive information should be involved in these operations in general.	Low
T	VI	6.1 Risk of high maintenance costs due to unreliable equipment	Moderate	unlikely	Economic impacts can appear when investment in this equipment is made and operations in the field are underwhelming or unreliable. Some of these devices and software can be expensive and certain maintenance operations may not be part of the regular warranty. These potential costs may be absorbed by the owner or user of the technology, depending on the type of technology ownership and use agreement. Hauler companies need to confirm maintenance costs and warranty terms to assure their operations budget covers these expenses. When a new vendor is needed, additional unplanned expenses can be required. Companies need to account for their return of investments	Low

B	RT	Risk description	Impact	Likelihood	Mitigation, comments, and strategies	Risk level
					and ongoing operations costs and life terms of these devices and software licenses.	
T	VI	6.2 Uninsured information management activities or use of AI may create unplanned costs	Moderate	unlikely	Certain cybersecurity insurance plans include new requirements for covering artificial intelligence solutions. This can increase insurance and, when not covered or reported, some insurance companies can drop coverage. This application is relatively simple one that avoids using more sophisticated AI solutions. The entity absorbing these costs, either the hauler companies or the City, needs to be sure that this application is also covered in their regular insurance or if there is any extra cost attached to it.	Low
T	VI	6.3 Risk of additional costs due to hidden licensing costs or changes in the technology vendor's terms on service	Moderate	Possible	Some technology vendors offer licensing tiers for their services and certain modules may require additional hidden fees to access them. They may include advanced image recognition features, hardware upgrades, or remote device access. Identify the needs for this project sooner than later and the entity responsible for the technology needs to make sure to understand licensing costs and be on top of terms of services changes.	Medium
U	IV	6.4 Risk of unplanned costs due to hauling companies staff training in new technology	Moderate	Possible	The implementation of this technology will need new processes in hauling companies to operate, manage, maintain, and supervise this technology. Some of these costs may not be considered as part of the initial budget for piloting or implementing this program. Consider working with technology vendors to assess the training needs and relying on existing expertise in the company to train staff and operators on information technology security and other aspects of best practices using these emerging tools.	Medium

Appendix A
Privacy risk assessment framework

Severity (Evaluate for the worst / highest possible impact)				
	A: Low	**B: Moderate**	**C: High**	**D: Extreme**
Individual Privacy Harms	Customer or "telephone book" information collected and could be disclosed (excluding utility customer data, protected by RCW)	Potential disclosure would be limited to non-financial, non-health related information; no personal identifiers (e.g., social security and driver's license #s)	Financial or other highly sensitive information would be collected and disclosable requiring action to remediate negative effects (example: non-HIPAA health data); i.e., credit report management required	Disclosure would result in extreme privacy impacts on highly regulated information; catastrophic public release of financial and personal information requiring credit report monitoring and other remediation
Equity, Disparate Community Impact	Little or no equity impact, technology delivered uniformly without reference to individuals or demographic groups	Accidental or perceived disparate impact to communities by nature of location of technology or service delivered	Intentional disparate equity impact resulting in community concern resulting in privacy harms, media coverage; loss of reputation, legitimacy and trust impacted	Extreme impacts to community, City experiences national media attention; widespread public concern and protest; significant breakdown in business processes associated with damage control
Political, Reputation & Image	Issues could be resolved internally by day-to-day processes; little or no outside stakeholder interest.	Issues could be raised by media and activist community resulting in protests and direct community complaints	Disclosure would likely result in heavy local media coverage; reputation, legitimacy and trust impacted	Likely national and international media coverage; serious public outcry; significant breakdown in business processes associated with mitigation and damage control
City Business, Quality & Infrastructure	Management of disclosure issues would represent negligible business interruption; resolved with no loss of productivity	Issue management would result in a brief loss of services; loss of < 1 week service delivery; limited loss of productivity	Significant event; loss of > 1–3-week loss of services; critical service interruption to delivery of infrastructure services	Extreme event; business collapse for department services; loss of > = 3 months of data or productivity; critical business infrastructure loss > 1 month
Legal & Regulatory	Adverse regulatory or legal action not indicated or highly unlikely	Relatively minor incident, regulatory action unlikely; possible legal intervention or consultation for addressing data exposure or loss	Adverse regulatory action likely – i.e., fines and actions associated with CJIS, HIPAA, PCI, NERC, COPPA violations, etc.	Major legislative or regulatory breach; investigation, fines, and prosecution likely; class action or other legal action

Financial Impact	$0-$500 impact; internal costs covered, and no significant external costs incurred	>$500 - $5,000; internal and external costs associated with legal consultation, system rework, overtime	> $5,000 -$50,000 external costs associated with fines, consultation fees and regulatory actions to mitigate information exposure; internal costs associated with system rework, overtime	> $50,000 external costs associated with fines, consultation fees and regulatory actions to mitigate information exposure; internal costs associated with system rework, overtime

Likelihood analysis.

For assessing probability of risks

Likelihood	Probability
Almost certain	Likely to occur yearly
Likely	Likely to occur every 2 years
Possible	Likely to occur every 5 years
Unlikely	Likely to occur every 10-20 years
Rare	It has never occurred

Risk Matrix

	Low	**Moderate**	**High**	**Extreme**
Almost Certain				**High**
Likely				
Possible		**Medium**		
Unlikely				
Rare	**Low**			

Appendix B
Definitions

Automated Decision System	A process, set of rules, or tool based on automated processing of data to perform calculations, create new data, or to undertake complex reasoning tasks. This includes advanced methods like artificial intelligence and machine learning, visual perception, speech or facial recognition, and automated translation between languages.
Data	Statistical, factual, quantitative, or qualitative information, in digital or analog form, that is regularly maintained or created by or on behalf of a City bureau and is in a form that can be transmitted or processed.
Data Governance	Definition of policies, processes and framework of accountability to appropriately manage data as a strategic asset.
Digital Age	This current era whereby social, economic and political activities are dependent on information and communication technologies. It is also known as the Information Age or the Digital Era.
Information	Information is the result of Data being processed, organized, structured or presented, allowing it to be used and understood.
Information Protection	A system of Data processing practices related to personally identifiable or identifying Data for the protection of privacy. This includes the management of individual pieces of personal Information, securing Data against unauthorized access, corruption or loss.
Metadata	A set of Data that describes and gives information about other Data, including its description, origination, and accuracy.
Open Data	Data that can be freely accessed, used, reused and redistributed by anyone.
Personal Information	Information about a natural person that is readily identifiable to that specific individual. "personal information," which include, but are not limited to: • identifiers such as a real name, alias, postal address, unique personal identifier, online identifier IP address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers; • payment card industry such as bank account numbers or access codes; • personal health data, such as health history, symptoms of a disease, current health care information, medical device identifiers and serial numbers; • commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies; • biometric information; • internet or other electronic network activity information, that includes browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement; • geolocation data, vehicle identifiers (including serial numbers and license plate numbers); • audio, electronic, visual, thermal, olfactory, or similar information; • professional or employment related information; • education information, provided that it is not publicly available; and • inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes
HRAR 11.04 Protection of Restricted and Confidential Information	
Privacy	The ability of an individual to be left alone, out of public view, and in control of information about oneself.

Confidential	Information that is made confidential or privileged by law or the disclosure of information that is otherwise prohibited by law or City policy.
Restricted	Some restrictions or limitations on the use of or disclosure of the information.
Principle of proportionality	The principle of proportionality requires that the processing of personal information must be relevant to, and must not exceed, the declared purpose
Surveillance Technologies	technologies that observe or analyze the movements, behavior, or actions of identifiable individuals in a manner that is reasonably likely to raise concerns about civil liberties, freedom of speech or association, racial equity or social justice.
Privacy terms	
Effectiveness	This refers to how a specific technology or solution fulfills the pursued objective.
Proportionality	Proportionality is a privacy principle that personal data collected and processed should be adequate, relevant, and limited to that necessary for purpose processed. Proportionality has multiple dimensions. Data collected and used should be adequate, because collecting too little information may lead to incorrect or incomplete information on a data subject. It should also be relevant and limited to what is necessary in relation to the purposes for which it is collected and processed (data minimization), both in terms of scope and time (data retention). The proportionality principles consideration of the amount of data to be collected. If excessive data is collected in relation to purposes, then it is disproportionate. Examples: Using biometric data like fingerprints to identify individuals when identity cards suffice.
Data protection	Data protection is the process of protecting data and involves the relationship between the collection and dissemination of data and technology, the public perception and expectation of privacy and the political and legal underpinning surrounding that data. It aims to strike a balance between individual privacy rights while still allowing data to be used for business purposes. Data protection is also known as data privacy or information privacy. Data protection should always be applied to all forms of data, whether it be personal or enterprise. It deals with both the integrity of the data, protection from corruption or errors, and privacy of data, it being accessible to only those that have access privilege to it.
Frequency of the collection	Periodicity of data collection.
Privacy safeguards	Measures are designed to improve privacy and information protection. It can be represented as below, as, or greater than industry standard and best practices
privacy fundamental rights	Privacy fundamental rights are set to help individuals in being assured of the protection and privacy of their personal data. The General Data Protection Regulation contains a set of 8 privacy fundamental rights. These rights are not legally binding in the US.
Right to information	This right provides the individual with the ability to ask for information about what personal data is being processed and the rationale for such processing. For example, a customer may ask for the list of processors with whom personal data is shared.
Right to access	This right provides the individual with the ability to get access to personal data that is being processed. This request provides the right for individuals to see or view their own personal data, as well as to request copies of the personal data.
Right to rectification	This right provides the individual with the ability to ask for modifications to personal data in case the individual believes that it is not up to date or accurate.

Right to withdraw consent	This right provides the individual with the ability to withdraw a previously given consent for processing of personal data for a purpose. The request would then require stopping the processing of personal data that was based on the consent provided earlier.
Right to object	This right provides the individual with the ability to object to the processing of their personal data. Normally, this would be the same as the right to withdraw consent if consent was appropriately requested and no processing other than legitimate purposes is being conducted. However, a specific scenario would be when a customer asks that their personal data should not be processed for certain purposes while a legal dispute is ongoing in court.
Right to object to automated processing	This right provides the individual with the ability to object to a decision based on automated processing. Using this right, a customer may ask for this request (for instance, a loan request) to be reviewed manually, because of the belief that automated processing of the loan may not consider the unique situation of the customer.
Right to be forgotten	Also known as the right to erasure, this right provides the individual with the ability to ask for the deletion of their data. This will generally apply to situations where a customer relationship has ended. It is important to note that this is not an absolute right and depends on your retention schedule and retention period in line with other applicable laws.
Right for data portability	This right provides the individual with the ability to ask for transfer of his or her personal data. As part of such a request, the individual may ask for their personal data to be provided back or transferred to another controller. When doing so, the personal data must be provided or transferred in a machine-readable electronic format.
Privacy risk	The term “privacy risk” means potential adverse consequences to individuals and society arising from the processing of personal data, including, but not limited to: 1. Direct or indirect financial loss or economic harm; 2. Physical harm; 3. Psychological harm, including anxiety, embarrassment, fear, and other demonstrable mental trauma; 4. Significant inconvenience or expenditure of time; 5. Adverse outcomes or decisions with respect to an individual’s eligibility for rights, benefits or privileges in employment (including, but not limited to, hiring, firing, promotion, demotion, compensation), credit and insurance (including, but not limited to, denial of an application or obtaining less favorable terms), housing, education, professional certification, or the provision of health care and related services; 6. Stigmatization or reputational harm; 7. Disruption and intrusion from unwanted commercial communications or contacts; 8. Price discrimination; 9. Effects on an individual that are not reasonably foreseeable, contemplated by, or expected by the individual to whom the personal data relate, that are nevertheless reasonably foreseeable, contemplated by, or expected by the covered entity assessing privacy risk, that significantly: A. Alters that individual’s experiences; B. Limits that individual’s choices; C. Influences that individual’s responses; or D. Predetermines results; or 10. Other adverse consequences that affect an individual’s private life, including private family matters, actions and communications within an individual’s home or similar physical, online, or digital location, where an individual has a reasonable expectation that personal data will not be collected or used. 11. Other potential adverse consequences, consistent with the provisions of this section, as determined by the Commission and promulgated through a rule.

Risk of individual privacy harms	The likelihood that individuals will experience harm or problems resulting from personal data collection and processing
Risk of equity, disparate community impact	The likelihood that specific groups will experience harm or problems resulting from the collection of multiple sources of personal data and their processing.
Risk of political, reputation & image issues	The likelihood that collection or processing of private data may result in harm on professional or personal relationships, harm in reputation or image.
Risk of city business, quality & infrastructure issues	The likelihood that the collection or processing of private data may impact or expose city relationships, agreements, or any other contract, or the quality of those businesses, or built infrastructure
Risk of legal & regulatory issues	The likelihood of any violation of existing laws or regulations by the collection or processing of private information
Risk of financial Impact	The likelihood that ongoing costs in management, collection or processing of private data may become financially inviable or present costs that may not be considered